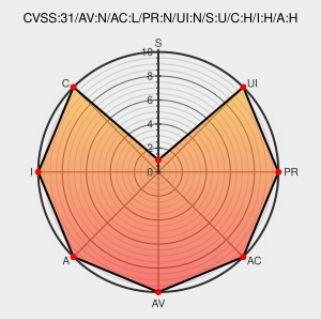
CVE-2021-28940

Published on: 04/02/2021 12:00:00 AM UTC

Last Modified on: 12/13/2022 04:34:00 PM UTC

CVE-2021-28940

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Magpierss from Magpierss Project contain the following vulnerability:

Because of a incorrect escaped exec command in MagpieRSS in 0.72 in the /extlib/Snoopy.class.inc file, it is possible to add a extra command to the curl binary. This creates an issue on the /scripts/magpie_debug.php and /scripts/magpie_simple.php page that if you send a specific https url in the RSS URL field, you are able to execute arbitrary commands.

CVE-2021-28940 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
magpierss/Snoopy.class.inc at 04d2a88b97fdba5813d01dc0d56c772d97360bb5	github.com text/html	MISC github.com/kellan/magpierss/blob/04d2a88b97fdba5813d01dc0d56c

· kellan/magpierss · GitHub		
MagpieRSS 0.72 - 'url' Command Injection and Server Side Request Forgery - PHP webapps Exploit	www.exploit-db.com Proof of Concept text/html	MISC www.exploit-db.com/exploits/49643
MagpieRSS 0.72 Command injection/code injection and Internal Server side request forgery. - Pastebin.com	pastebin.com text/html	MISC pastebin.com/kpzHKKJu

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Magpierss Project	Magpierss	0.72	All	All	All

cpe:2.3:a:magpierss_project:magpierss:0.72:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-28940 : Because of a incorrect escaped exec command in MagpieRSS in 0.72 in the /extlib/Snoopy.class.inc f… twitter.com/i/web/status/1…	2021-04-02 20:04:22
@LinInfoSec	Php - CVE-2021-28940: github.com/kellan/magpier…	2021-04-02 23:25:14
/r/netcve	CVE-2021-28940	2021-04-02 20:36:18

← Previous ID Next ID→

CVE.report and Source URL Uptime Status status.cve.report